UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA

Jonathan Torres, individually and on behalf of all others similarly situated,

Plaintiff,

v.

The Wendy's Company,

Defendant.

Case No. 6:16-cv-210-Orl-18DAB

CLASS ACTION COMPLAINT

Jury Trial Demanded

CLASS ACTION COMPLAINT

Plaintiff Jonathan Torres, by and through his undersigned counsel, bring this Class Action Complaint against The Wendy's Company, on behalf of himself and all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff bring this class action against The Wendy's Company (referred to herein as "Wendy's" or "Defendant") for its failure to secure and safeguard its customers' credit and debit card numbers and other payment card data ("PCD"), and other personally identifiable information which Wendy's collected at the time Plaintiff made a purchase of food items at one its restaurants ("PII") (collectively, "Private Information"), and for failing to provide timely, accurate and adequate notice to Plaintiff and other Class members that their Private Information had been stolen and precisely what types of information were stolen.

2. Beginning at a point in time presently unknown, hackers utilizing malicious malware accessed the computer systems at Wendy's locations throughout the United States,

including locations in this District, and stole copies of Wendy's customers' Private Information (the "Data Breach").

3. On January 27, 2016, Wendy's announced that it had discovered malicious software designed to steal credit card and debit card data on computers that operate the payment processing systems for its restaurants. Wendy's released very few details, nor did it explain why it had delayed notification of the public through a press release of the Data Breach. In its press release, Wendy's acknowledged the weakness of its security system at the time of the Data Breach, and that since the Data Breach it had taken steps to strengthen the security of its systems. Unfortunately, Wendy's did not explain why such security measures had not already been in place at the time of the Data Breach to prevent the loss of Plaintiff's and class members' PII.

4. Wendy's could have prevented this Data Breach. The malicious software used in the Data Breach was more than likely a variant of "BlackPOS," the identical malware strain that hackers used in last year's data breach at many other retail establishments. While many retailers, banks and card companies responded to recent breaches by adopting technology that helps makes transactions more secure, Wendy's has acknowledged that it has retained a security consultant to review and look into its systems. The quality of the measures in place are suspect and the need for judicial intervention and consumer and independent oversight is mandated by the circumstances described herein.

5. Wendy's disregarded Plaintiff's and Class members' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, and failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' Private Information.

On information and belief, Plaintiff's and Class members' Private Information was improperly handled and stored, was unencrypted, and was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiff's and Class members' Private Information was compromised and stolen. However, as this same information remains stored in Wendy's computer systems, Plaintiff and class members have an interest in ensuring that their information is safe, and they should be entitled to seek injunctive and other equitable relief, including independent oversight of Wendy's security systems.

PARTIES

6. Plaintiff, Jonathan Torres, is a resident of the state of Florida. On January 3, 2016, Plaintiff Jonathan Torres visited a Wendy's restaurant in Orlando, Florida and purchased food items using his debit card issued by his credit union. Shortly thereafter, and while his debit card (and pin number) was in his possession, Plaintiff was contacted by his credit union and he discovered while speaking with a representative of his credit union that his debit card number had been used to make a purchase at a Sport's Authority in the amount of $200, and $377.74 at a Best Buy store. Neither one of these transactions had been made or authorized by Plaintiff, and they were made by the person or persons who stole his debit card number from Wendy's. These transactions were not made or authorized by Plaintiff, and were made even though he had physical possession of his debit card at the time these fraudulent transactions were made. Plaintiff has reported the theft to his credit union and local law enforcement.

7. The Wendy's Company (NASDAQ: WEN) is the world's third largest quick-service hamburger company. The Wendy's system includes approximately 6,500 franchise and Company restaurants in the U.S., 29 other countries, and U.S. territories worldwide. Its revenues in 2014 totaled $2.1 billion. Among the restaurants, it operates or controls are restaurants in this

its filings with the Securities Exchange Commission the problems inherent with the collection of information from consumers. Specifically, it has stated:

> We rely on computer systems and information technology to run our business. Any material failure, interruption or security breach of our computer systems or information technology may result in adverse publicity and adversely affect the operation of our business and results of operations. We are significantly dependent upon our computer systems and information technology to properly conduct our business. A failure or interruption of computer systems or information technology could result in the loss of data, business interruptions or delays in business operations. Also, despite our considerable efforts and technological resources to secure our computer systems and information technology, security breaches, such as unauthorized access and computer viruses, may occur resulting in system disruptions, shutdowns or unauthorized disclosure of confidential information. A significant security breach of our computer systems or information technology could require us to notify customers, employees or other groups, result in adverse publicity, loss of sales and profits, and incur penalties or other costs that could adversely affect the operation of our business and results of operations.
>
> Failure to comply with laws, regulations and third-party contracts regarding the collection, maintenance and processing of information may result in adverse publicity and adversely affect the operation of our business and results of operations.
>
> We collect, maintain and process certain information about customers and employees. Our use and protection of this information is regulated by various laws and regulations, as well as by third-party contracts. If our systems or employees fail to comply with these laws, regulations or contract terms, it could require us to notify customers, employees or other groups, result in adverse publicity, loss of sales and profits, increase fees payable to third parties, and incur penalties or remediation and other costs that could adversely affect the operation of our business and results of operations.

12. When consumers make purchases at Wendy's restaurants they typically pay for their purchases using credit or debit cards, and Wendy's collects PCD related to that card including the card holder name, the account number, expiration date, card verification value (CVV), and PIN data for debit cards. Wendy's stores the PCD in its point-of-sale system and transmits this information to a third party for completion of the payment.

B. Stolen Private Information Is Valuable to Hackers and Thieves

13. It is well known and the subject of many media reports that PII data is highly coveted and a frequent target of hackers. PII data is often easily taken because it may be less protected and regulated than payment card data. In the hospitality industry and as identified earlier, a large number of fast food chains were the targets of data breaches. Despite the frequent public announcements of data breaches by retailers, Wendy's opted to maintain an insufficient and inadequate system to protect the PII of Plaintiff and class members.

14. Legitimate organizations and the criminal underground alike recognize the value in PII. Otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data from 38 million users."1 Similarly, in the Target data breach, in addition to PCI data pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 customers.

15. Biographical data is also highly sought after by data thieves. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." Id. PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of thefts and unauthorized access have been the subject of many media reports. One form of identity theft has been branded as "synthetic identity theft," and occurs when thieves create new identities by combining real and fake identifying information then using those identities to open new accounts. "This is where they'll take your Social Security number, my name and address, someone else's birthday and they will combine them into the equivalent of

---

[1] Verizon 2014 PCI Compliance Report, available at <http://www.nocash.info.ro/wp-content/uploads/2014/02/ Verizon_pci-report-2014.pdf> (hereafter "2014 Verizon Report"), at 54 (last visited Sept. 24, 2014).

District, including the one referred to in the preceding paragraph. Wendy's is incorporated in Delaware, and maintains its headquarters in Dublin, Ohio and is authorized to do business in this state.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed $5,000,000, exclusive of interest and costs, and this is a class action in which more than two-thirds of the proposed plaintiff class, on the one hand, and Wendy's, on the other, are citizens of different states.

9. This Court has jurisdiction over Wendy's as it operates restaurants serving the public, and it is at one of the restaurants in this District that Plaintiff made a purchase using his debit card which led to the damages which he suffered. Wendy's also advertises in a variety of media throughout the United States, including Florida and this District. Through its business operations in this District, Wendy's intentionally avails itself and markets its restaurants within this District to render the exercise of jurisdiction by this Court just and proper.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District and as Wendy's operates restaurants within this District.

FACTUAL BACKGROUND

A. Wendy's and Its Private Information Collection Practices

11. Wendy's primarily derives its revenues from restaurant operations, management and franchise fees and other revenues. In connection with its operations, it has acknowledged in

a bionic person," said Adam Levin, chairman of IDT911, which helps businesses recover from identity theft. Synthetic identity theft is harder to unravel than traditional identity theft, experts said. "It's tougher than even the toughest identity theft cases to deal with because they can't necessarily peg it to any one person," Levin has said. In fact, the fraud might not be discovered until an account goes to collections and a collection agency researches the Social Security number.

16. Unfortunately, and as is alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, such as retailers, Wendy's approach at maintaining the privacy of Plaintiff's and Class members' PII was lackadaisical, cavalier, reckless, or at the very least, negligent.

C. Wendy's Failed to Segregate PCD From PII

17. Unlike PII data, PCD (or payment card data) is heavily regulated. The Payment Card Industry Data Security Standard ("PCI DSS") is a set of requirements designed to ensure that companies maintain consumer credit and debit card information in a secure environment.

18. "PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data."[2]

19. One PCI requirement is to protect stored cardholder data. Cardholder data includes Primary Account Number, Cardholder Name, Expiration Date, and Service Code. "Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement."[3] However, segregation is

[2] PCI DSS v. 2 at 5 (2010) (hereafter PCI Version 2).
[3] *Id.* at 10.

recommended because among other reasons, "[i]t's not just cardholder data that's important; criminals are also after personally identifiable information (PII) and corporate data."[4]

20. Illicitly obtained PII and PCI, sometimes aggregated from different data breaches, is sold on the black market, including on websites, as a product at a set price.[5]

D. The 2016 Data Breach at Wendy's

21. On January 27, 2016, Wendy's disclosed in a press releases (but not posted as of February 5, 2016 on its web site) that it had recently discovered malicious software designed to steal credit and debit card data on computers that operate the payment processing systems for Wendy's restaurants .

22. Wendy's has not indicated whether other information provided by consumers or location information, were disclosed in the breach. Moreover, it has done little beyond a press release to notify consumers of the Data Breach.

23. Without such detailed disclosure, Plaintiff and Class members are unable to take the necessary precautions to prevent imminent harm, such as continued misuse of their personal information.

24. Wendy's has failed to provide a cogent picture of how the Data Breach occurred and its full effects on consumers' PII and PCD information.

25. Hacking is often accomplished in a series of phases to include reconnaissance, scanning for vulnerabilities and enumeration of the network, gaining access, escalation of user, computer and network privileges, maintaining access, covering tracks and placing backdoors.

---

[4] *See* Verizon Report at 54.

[5] *See, e.g.*, <http://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth> (last visited Sept. 24, 2014).

On information and belief, while hackers scoured Wendy's networks to find a way to access PCD, they had access to and collected the PII stored on Wendy's networks.

26. Thieves already are using the Private Information stolen from Wendy's to commit actual fraud, as occurred to Plaintiff as alleged herein.

27. The Data Breach was caused and enabled by Wendy's knowing violation of its obligations to abide by best practices and industry standards in protecting its customers' Private Information.

28. In this regard, more than likely the software used in the attack was a variant of "BlackPOS," a malware strain designed to siphon data from cards when they are swiped at infected point-of-sale systems. Hackers had previously utilized BlackPOS in other recent cyber-attacks, including breaches at Home Depot and Target. While many retailers, banks and card companies have responded to these recent breaches by adopting technology and security practices that help makes transactions and stored data more secure, Wendy's has acknowledged that it did not do so.

E. This Data Breach Will Result Additional In Identity Theft and Identify Fraud

29. Wendy's failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the data breach.

30. The ramifications of Wendy's failure to keep Plaintiff's and Class members' data secure are severe.

31. The information Wendy's compromised, including Plaintiff's identifying information and/or other financial information, is "as good as gold" to identity thieves, in the

words of the Federal Trade Commission ("FTC").[6] Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes. The FTC estimates that as many as 10 million Americans have their identities stolen each year.

32. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account (as occurred to Plaintiff here) , run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[7]

33. According to Javelin Strategy and Research, "1 in 4 data breach notification recipients became a victim of identity fraud."[8] Nearly half (46%) of consumers with a breached debit card became fraud victims within the same year.

34. Identity thieves can use personal information such as that of Plaintiff and Class members, which Wendy's failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years. The IRS paid out 43.6 billion in potentially fraudulent

---

[6] FTC Interactive Toolkit, Fighting Back Against Identity Theft, *available at* http://www.dcsheriff.net/community/documents/id-theft-tool-kit.pdf (last visited Sept. 24, 2014).

[7] FTC, Signs of Identity Theft, available at <http://www.consumer.ftc.gov/articles/ 0271-signs-identity-theft> (last visited Sept. 24, 2014).

[8] See 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, available at <www.javelinstrategy.com/brochure/ 276> (last visited Sept. 24, 2014) (the "2013 Identity Fraud Report").

returns in 2012, and the IRS identified more than 2.9 million incidents if identity theft in 2013. The IRS has described identity theft as the number one tax scam for 2014.

35. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[9] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." Id. at 11.

F. Annual monetary losses from identity theft are in the billions of dollars.

36. Javelin Strategy and Research reports that those losses increased to $21 billion in 2013.[10]

37. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

38. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges

---

[9] Victims of Identity Theft, 2012 (Dec. 2013) at 10, available at <http://www.bjs.gov/content/pub/pdf/vit12. pdf> (last visited Sept. 24, 2014).

[10] *See* 2013 Identity Fraud Report.

[11] GAO, Report to Congressional Requesters, at p.33 (June 2007), available at <http://www.gao.gov/new.items/d07737.pdf> (emphases added) (last visited Sept. 24, 2014).

incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

G. Plaintiff and Class Members Suffered Damages

39. The Data Breach was a direct and proximate result of Wendy's failure to properly safeguard and protect Plaintiff's and Class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Wendy's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

40. Plaintiff's and Class members' PII is private and sensitive in nature and was left inadequately protected by Wendy's. Wendy's did not obtain Plaintiff's and Class members' consent to disclose their PII to any other person as required by applicable law and industry standards.

41. As a direct and proximate result of Wendy's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

42. Wendy's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' Private Information,

causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their credit/debit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the Internet card black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their Private Information;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;

h. overpayments to Wendy's for products and services purchased during the Data Breach in that a portion of the price paid for such products and services by Plaintiff and Class members to Wendy's was for the costs of reasonable and adequate safeguards and security measures that would protect customers' Private Information, which Wendy's did not implement and, as a result, Plaintiff and Class members did not receive what they paid for and were overcharged by Wendy's;

i. the loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts; and

j. deprivation of rights they possess under the Florida Deceptive and Unfair Trade Practices Act (FDUTPA);

k. Plaintiff's economic injury is also described in Paragraph 8.

43. Acknowledging the repercussions from its wrongful actions and inaction and the resulting Data Breach, Wendy's has offered its customers only one year of credit monitoring and identity theft protection services, despite the fact that it is well known, and acknowledged by government that damage and fraud from a data breach can take years to occur. Wendy's has instead opted to save the cost of such services to ensure its profits remain unaffected by limiting this protection to only one year. As a result, Plaintiff and class members' are left to their own actions to protect themselves from the financial carnage Wendy's has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Wendy's has placed Plaintiff and Class members in, is ascertainable and is a determination appropriate for the trier of fact. Wendy's has also not offered to cover any of the damage sustained by Plaintiff or class members.

44. While the Private Information of Plaintiff and members of the Class has been stolen, the same or a copy of the Private Information continues to be held by Wendy's. Plaintiff and members of the Class have an undeniable interest in insuring that this information is secure, remains secure, and not subject to further theft.

CLASS ACTION ALLEGATIONS

45. Plaintiff seeks relief in her individual capacity and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2) , (b)(3) and (c)(4), Plaintiff seeks certification of a Nationwide class and a Florida class. The national class is initially defined as follows:

46. All persons residing in the United States whose personal and/or financial information was disclosed in the data breach affecting Wendy's in 2015 (the "Nationwide Class").

47. The Florida Class is initially defined as follows: All persons residing in Florida whose personal and/or financial information was disclosed in the data breach affecting Wendy's in 2015 (the "Florida Class).

48. Excluded from each of the above Classes are Wendy's, including any entity in which Wendy's has a controlling interest, is a parent or subsidiary, or which is controlled by Wendy's, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Wendy's. Also excluded are the judges and court personnel in this case and any members of their immediate families.

49. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, Wendy's has acknowledged that debit and credit cards were affected by the breach at many of its restaurants in the United States, including the one where Plaintiff dined.

50. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Wendy's violated the Florida Deceptive and Unfair Trade Practices Act (FDUTPA) by failing to implement reasonable security procedures and practices;

b. Whether Wendy's violated FDUTPA by failing to promptly notify class members their personal information had been compromised;

c. Whether class members may obtain an injunctive relief against Wendy's under FDUTPA to require that it safeguard, or destroy rather than retain the Private Information of Plaintiff and Class members;

d. What security procedures and data-breach notification procedure should Wendy's be required to implement as part of any injunctive relief ordered by the Court;

e. Whether Wendy's has an implied contractual obligation to use reasonable security measures;

f. Whether Wendy's has complied with any implied contractual obligation to use reasonable security measures;

g. What security measures, if any, must be implemented by Wendy's to comply with its implied contractual obligations;

h. Whether Wendy's violated FDUTPA in connection with the actions described herein; and

i. The nature of the relief, including equitable relief, to which Plaintiff and the Class members are entitled.

51. All members of the purposed Classes are readily ascertainable. Wendy's has access to addresses and other contact information for millions of members of the Classes, which can be used for providing notice to many Class members.

52. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class members because Plaintiff's information, like that of every other class member, was misused and/or disclosed by Wendy's.

53. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation.

54. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

55. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Wendy's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

56. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Wendy's has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

COUNT I
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

57. Plaintiff incorporates the substantive allegations contained in Paragraphs 1 through 56 as if fully set forth herein.

58. Wendy's solicited and invited Plaintiff and Class members to eat at its restaurants and make purchases using their credit or debit cards. Plaintiff and Class members accepted Wendy's offers and used their credit or debit cards to make purchases at Wendy's restaurants during the period of the Data Breach.

59. When Plaintiff and Class members made and paid for purchases of Wendy's services and products in connection with their meals at Wendy's properties, they provided their PII and PCD, including but not limited to the PII and PCD contained on the face of, and embedded in the magnetic strip of, their debit and credit cards. In so doing, Plaintiff and Class members entered into implied contracts with Wendy's pursuant to which Wendy's agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members if their data had been breached and compromised.

60. Each purchase at a Wendy's restaurants made by Plaintiff and Class members using their credit or debit card was made pursuant to the mutually agreed-upon implied contract with Wendy's under which Wendy's agreed to safeguard and protect Plaintiff's and Class members' PII and PCD, including all information contained in the magnetic stripe of Plaintiff's and Class members' credit or debit cards, and to timely and accurately notify them if such information was compromised or stolen.

61. Plaintiff and Class members would not have provided and entrusted their PII and PCD, including all information contained in the magnetic stripes of their credit and debit cards,

to Wendy's to eat at its restaurants and make purchases in the absence of the implied contract between them and Wendy's.

62. Plaintiff and Class members fully performed their obligations under the implied contracts with Wendy's.

63. Wendy's breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the PII and PCD of Plaintiff and Class members and by failing to provide timely and accurate notice to them that their PII and PCD was compromised in and as a result of the Data Breach.

64. As a direct and proximate result of Wendy's breaches of the implied contracts between Wendy's and Plaintiff and Class members, Plaintiff and Class members sustained actual losses and damages as described in detail above.

COUNT II
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

65. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 56 as if fully set forth in this Count.

66. Upon accepting and storing Plaintiff's and Class Members' Private Information in their respective computer database systems, Wendy's undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to utilize commercially reasonable methods to do so. Wendy's knew, acknowledged and agreed that the Private Information was private and confidential and would be protected as private and confidential.

67. The law imposes an affirmative duty on Wendy's to timely disclose the unauthorized access and theft of the Private Information to Plaintiff and the Class so that

Plaintiff and Class Members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

68. Wendy's breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting many months after learning of the breach to notify Plaintiff and Class Members and then by failing to provide Plaintiff and Class Members any information regarding the breach until December 2015, and January 2016. To date, Wendy's has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

69. Wendy's also breached its duty to Plaintiff and the Class Members to adequately protect and safeguard this information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, Wendy's failed to provide adequate supervision and oversight of the Private Information with which it is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to gather Plaintiff's and Class Members' Private Information, misuse the Private Information and intentionally disclose it to others without consent.

70. Through Wendy's acts and omissions described in this Complaint, including Wendy's failure to provide adequate security and its failure to protect Plaintiff's and Class Members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Wendy's unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' Private Information during the time it was within Wendy's possession or control.

71. Further, through its failure to provide timely and clear notification of the data breach to consumers, Wendy's prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

72. Upon information and belief, Wendy's improperly and inadequately safeguarded Private Information of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access.

73. Wendy's failure to take proper security measures to protect Plaintiff's and Class Members' sensitive Private Information as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class Members' Private Information.

Wendy's failed to take proper security measures to protect Plaintiff's and Class Members' sensitive Private Information.

74. Wendy's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Private Information; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class Members' Private Information; and failing to provide Plaintiff and Class Members with timely and sufficient notice that their sensitive Private Information had been compromised.

75. Neither Plaintiff nor the other Class Members contributed to the data breach and subsequent misuse of their Private Information as described in this Complaint.

76. As a direct and proximate cause of Wendy's conduct, Plaintiff and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the

Private Information of Plaintiff and Class Members and/or filing false tax returns; and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT III
Violations of Florida's Unfair and Deceptive Trade Practices Act
(On behalf of Plaintiff and the Florida Class)

77. Plaintiff repeats and incorporates the allegations contained in paragraphs 1 through 56 as if fully set forth in this Count.

78. The Florida Unfair and Deceptive Trade Practices Act (hereinafter "FUDTPA") is expressly intended to protect "consumers" like Plaintiff and Class Members from unfair or deceptive trade practices.

79. Plaintiff and Class Members have a vested interest in the privacy, security and integrity of their Private Information, therefore, this interest is a "thing of value" as contemplated by FUDTPA.

80. Wendy's is a "person" within the meaning of the FUDTPA and, at all pertinent times, was subject to the requirements and proscriptions of the FUDTPA with respect to all of their business and trade practices described herein.

81. Plaintiff and Class Members are "consumers" "likely to be damaged" by Wendy's ongoing deceptive trade practices.

82. Wendy's unlawful conduct as described in this Complaint, was facilitated, directed, and emanated from Wendy's headquarters to the detriment of Plaintiff and Class Members.

83. Wendy's engaged in unfair and deceptive trade practices by holding itself out as providing as secure online environment and by actively promoting trust online with consumers, which created in consumers' minds a reasonable expectation of privacy to all consumers by promising that consumers' Private Information is safe with Wendy's, but then failed to take commercially reasonable steps to protect the Private Information with which it is entrusted.

84. Wendy's violated FUDTPA by failing to properly implement adequate, commercially reasonable security measures to protect consumers' sensitive Private Information.

85. Wendy's also violated FUDTPA by failing to immediately notify affected Plaintiff and Class Members of the nature and extent of the data breach.

86. Wendy's acts, omissions and conduct also violate the unfair component of FUDTPA because Wendy's acts, omissions and conduct, as alleged herein, offended public policy and constitutes immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and other Class members. The gravity of Wendy's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Wendy's legitimate business interests, other than Wendy's conduct described herein.

87. Wendy's failed to properly implement adequate, commercially reasonable security measures to hold this information in strict confidence, failed to safeguard Plaintiff's and Class members' Private Information, and failed to protect against the foreseeable loss and misuse of this information.

88. Plaintiff and Class members have suffered ascertainable losses as a direct result of Wendy's employment of unconscionable acts or practices, and unfair or deceptive acts or practices.

89. By failing to disclose that it does not enlist industry standard security practices, which render Wendy's products and services particularly vulnerable to data breaches, Wendy's engaged in a deceptive business practice that is likely to deceive a reasonable consumer.

90. A reasonable consumer would not have made purchases at a Wendy's restaurants with a credit or debit card had she known the truth about Wendy's security procedures. By withholding material information about Wendy's security practices, Wendy's was able to convince customers to provide and entrust their Private Information to Wendy's. Had Plaintiff known truth about Wendy's security procedures, she would not have dined at Wendy's.

91. Wendy's failure to disclose that it does not enlist industry standard security practices also constitutes an unfair business practice under the FDUTPA. Wendy's conduct is unethical, unscrupulous, and substantially injurious to the Florida Class. Whereas Wendy's competitors have spent the time and money necessary to appropriately safeguard their products, service, and customer information, Wendy's has not—to the detriment of its customers and to competition.

92. As a result of Wendy's violations of the FDUTPA, Plaintiff and the other members of the Florida class are entitled to injunctive relief including, but not limited to: (1) ordering that Wendy's utilize strong industry-standard encryption algorithms for encryption keys that provide access to stored customer data; (2) ordering that Wendy's implement the use of its encryption keys in accordance with industry standards; (3) ordering that Wendy's, consistent with industry standard practices, engage third party security auditors/penetration testers as well

as internal security personnel to conduct testing, including simulated attacks, penetration tests and audits on Wendy's systems on a periodic basis; (4) ordering that Wendy's engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Wendy's audit, test and train its security personnel regarding any new or modified procedures; (6) ordering that Wendy's, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Wendy's is compromised, hackers cannot gain access to other portions of Wendy's systems; (7) ordering that Wendy's purge, delete, destroy in a reasonable secure manner customer data not necessary for its provisions of services; (8); ordering that Wendy's, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that Wendy's, consistent with industry standard practices, evaluate web applications for vulnerabilities to prevent web application threats to consumers who eat at Wendy's or make purchases through the internet; (10) ordering that Wendy's, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (11) ordering Wendy's to meaningfully educate its customers about the threats they face as a result of the loss of their Private Information to third parties and the theft of Wendy's source code, as well as the steps Wendy's customers must take to protect themselves.

93. As a result of Wendy's violations of the FDUTPA, Plaintiff and Class members have suffered injury in fact and lost money or property, as detailed above. Plaintiff ate at a Wendy's restaurants and purchased products or services she otherwise would not have purchased or paid for. Plaintiff requests that the Court issue sufficient equitable relief to restore

Class members to the position they would have been in had Wendy's not engaged in unfair competition, including by ordering restitution of all funds that Wendy's may have acquired as a result of its unfair competition.

94. Under FDUPTA, Plaintiff and the Class are entitled to preliminary and permanent injunctive relief without proof of monetary damage, loss of profits, or intent to deceive. Plaintiff and the Class seek equitable relief and to enjoin Wendy's on terms that the Court considers appropriate.

95. Wendy's conduct caused and continues to cause substantial injury to Plaintiff and Class Members. Unless preliminary and permanent injunctive relief is granted, Plaintiff and the Class will suffer harm, Plaintiff and the Class Members do not have an adequate remedy at law, and the balance of the equities weighs in favor of Plaintiff and the Class.

96. At all material times, Wendy's deceptive trade practices are willful within the meaning of FUDTPA and, accordingly, Plaintiff and the Class are entitled to an award of attorneys' fees, costs and other recoverable expenses of litigation.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Wendy's as follows:

a. For an Order certifying the Nationwide Class and Florida Class as defined herein , and appointing Plaintiff and their Counsel to represent the Nationwide Class and Florida Class;

b. For equitable relief enjoining Wendy's from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff and Class

members' private information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiff and Class members;

c. For equitable relief compelling Wendy's to utilize appropriate methods and policies with respect to consumer data collection, storage and safety and to disclose with specificity to Class members the type of PII and PCD compromised.

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Wendy's wrongful conduct;

e. For an award of actual damages, compensatory damages, in an amount to be determined;

f. For an award of costs of suit and attorneys' fees, as allowable by law; and

g. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

Dated: February 8, 2016

Respectfully submitted,

JOHN A. YANCHUNIS
Florida Bar No. 324681
PATRICK A. BARTHLE, II
Florida Bar No. 99286
MARCIO W. VALLADARES
Florida Bar No. 986917
PAUL L. SANGIOVANNI
Florida Bar No. 513164
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jyanchunis@ForThePeople.com